[一般論文]ハッキング行為が正当化される条件

AUTHOR(S):

北島, 雄一郎

CITATION:

北島, 雄一郎. [一般論文]ハッキング行為が正当化される条件. 京都大学文学部哲学研究室紀要 2011, 14: 69-80

ISSUE DATE:

2011

URL:

http://hdl.handle.net/2433/173149

ハッキング行為が正当化される条件

北島雄一郎

1. はじめに

カリフォルニア州マウンテンビューにあるグーグル本社近くに‘Hacker Dojo’があるという。これは、開発したソフトウェアやサービスについて語り合い、切磋琢磨する非営利組織（NPO）の本拠地である。その理事の一人は、ハッカーについて「技術者の間では深い知識を持つ専門家をハッカーと呼び、不正行為をするクラッカーと区別します。日本の空手道場のようにハッカーが技を究める鍛錬の場にしたいのです」と語っている(1)。このように、一般に「ハッカー」は、悪意によってコンピュータシステムに侵入する「クラッカー」とは区別されており、優れた性質に対する肯定的な評価を含んでいる。つまり、「勇者」や「やさしい」といった言葉と同様、単にある性質を記述している言葉ではなく、価値評価を含む言葉である(江口, 2000, 172-173 頁)。しかし、本稿では「ハッカー」という言葉にこうした価値評価を含まず、単にコンピュータシステムに侵入する人という意味で用い、コンピュータシステムへ侵入することを、ハッキング行為とよぶ。こうした行為は正当化されるのだろうか、されるとしたらどのような条件をみたしたときなのか。これが本稿で考えたい問題である。

この問題を考える前に、「不正」という言葉について簡単に注意しておこう。本稿では「不正」という言葉を使うとき、法律的な意味での不正ではなく、道徳的な意味での不正として用いる。例えば、人種差別を容認する法律があったとすると、この法律を破ることは法律的には正しくないが、道徳的には不正でないかもしれない。

また、こうした問題設定に対して、次のような反論が考えられる。そもそも現実社会において不法侵入は、その行為によって害を及ぼそうと及ぼさなかろうと、道徳的に許される行為ではない。同様に、ハッキング行為も、その行為によって害を及ぼそうと及ぼさなかろうと、道徳的に許される行為ではない。したがって、ハッキング行為が許されるかどうかという問題に対する答えは自明であり、ハッキング行為は道徳的に許される行為ではない。

しかし、この議論には、二つの問題点がある(Himma, 2008, pp. 192-193)。一つは、ハッキング行為が不法侵入の一種であるとしても、すべてのハッキング行為が不正であるということにはならないということである。なぜなら、すべての不法侵入が道徳的に不正である

とは限らないからだ。例えば、ある家にその家の住人を殺そうと押し入ってきた人を、他の人がその行為を阻止しようとしてその家に侵入したとしても、その行為を直ちに不正であると判断することは難しい。二つめの問題点は、不法侵入という概念をコンピュータシステムへの侵入に適用できるかどうかはっきりしないことである。ハッキングは他人のコンピュータシステムへ物理的に侵入するわけではない。つまり、現実社会における不法侵入との単純なアナロジーは成立しない。コンピュータ技術という新しい技術が現れたことに伴い、それ以前の道徳的な指針を単純に適用できないような指針の空白（policy vacuums）が生じているのだ(Moor, 2001)。

このように、コンピュータへの不法侵入が不正であるかどうかというのは、自明の問題ではない。そこで、本稿では、どのような条件のもとでコンピュータへの不法侵入が正当化されるのかという問題を考える。この問題を考えるとき、どのような倫理的立場で考えるかをはっきりさせておく必要があるだろう。ある行為が正しいか不正であるかという問題に対しては、いくつかの立場が考えられるが、その中には例えば義務論や帰結主義といった立場がある。義務論の立場では、ある行為の帰結に関係なく、その行為の性質によって、その行為が正しいか不正であるかを判断する。例えば、この立場では、「嘘をつく」という行為の性質を吟味して、この行為が不正であると判断したならば、この行為がどのような帰結を導こうとも、この行為は不正であることになる。一方、帰結主義はある行為が正しいか不正であるかは、その行為の性質ではなく、その行為がもたらす帰結をもとに判断する。例えば、「嘘をつく」という行為も、望ましい帰結をもたらすのであれば、この行為は正しいことになる。

Spafford(1992, pp. 41-42)は、ある行為がどのような帰結をもたらすのかを判断することが難しいという理由から、義務論的な立場からシステムに侵入するという行為が正当化されるかどうかを検討した。しかし、江口(2000)が指摘しているように、Spafford(1992)は義務論の立場に立つと述べているものの、帰結主義的な議論を行なっている場合もある。義務論の立場が妥当であるか、帰結主義の立場が妥当であるかという問題は、重要な問題であるけれども、本稿ではその問題には立ち入らず、帰結主義の立場に立って議論することにする。

Manion & Goodrum(2000)は、いくつかの条件を満足している場合、ハッキング行為が正当化される場合もあると論じた。本稿では、Spafford(1992)によるハッキング行為に関する議論を参照しながら、Manion & Goodrum(2000)の議論を検討したい。そのためにまず 2 節で帰結主義の観点から Spafford(1992)の議論を概観し、3 節で Manion & Goodrum(2000)の議

論を考察する。そしてこの考察をもとに、ハッキング行為が正当化されることは皆無に近いと結論する。

2. Spafford(1992)の議論

Spafford(1992)は、ハッキング行為を正当化する議論をいくつか取り上げ、どれも妥当でないと論じた。この節では、これらの議論とそれに対する Spafford(1992)の批判を帰結主義の立場から概観する。

2.1 情報はフリーであるべきという議論

ハッカーは「情報はフリーである」という見解を根拠として、自分の行動を正当化することがある。この見解によれば、情報は万人のためのものであり、情報へのアクセスに制限を設けるべきではない。しかし、このような見解のもとでは、いくつかの問題が生じる(Spafford, 1992, pp. 42-43)。一つは、プライバシーの問題である。すべての情報にアクセス可能であるならば、個人のクレジットカードの情報にアクセスできることになり、プライバシーは全くないことになってしまう。もう一つの問題は、情報の信頼性に関する問題である。すべての情報にアクセスできるのであれば、医療記録やクレジットカードの情報をコントロールできなくなり、そうした情報の信頼性が失われてしまう。

この議論を帰結主義の観点から言い換えると、情報をフリーであるとすることによってもたらされる良い帰結が、プライバシーや情報の信頼性が失われてしまうという情報をフリーに扱うことによってもたらされる悪い帰結を上回るとは考えられないということになる。

2.2 セキュリティの議論

ハッカーがシステムに侵入することによって、システムの弱点が明らかになるのだから、ハッキング行為は正当化されるとする議論もある。しかし、この議論も Spafford(1992, pp. 43-44)によれば、説得力がない。ハッカーがシステムの弱点を発見してシステムに侵入することができるのならば、侵入するのではなくシステムの管理者に直接その弱点を伝えればよい。例えば、ショッピングモールの防火システムの欠陥を指摘するために、放火することは道徳的に許されることではないだろう。

この議論のもう一つの問題点は、多くのウェブサイトの管理者にとって、その弱点を常に修正して最新の状態に保つということは、多大な負担がかかるということを考慮していないということである。つまり、システムの管理者の、技術的、経済的な状況を考えてい

ないのだ。例えば、最新鋭の防犯システムが整備されていない家に泥棒が入った場合、その家の人が、最新鋭の防犯システムを整備していなかったからといって、自業自得ということにはならないだろう。

この議論も、帰結主義的なものである(江口, 2000, 181 頁)。明示的に述べると、ハッキング行為によってセキュリティの欠陥が明らかになるという良い帰結より、ハッキング行為によってウェブサイトの管理者に多大な労力をかけるという悪い帰結のほうが上回るということになる。

2.3 使用されていないシステムの議論

ハッカーは単に使用されていないシステムを有効利用しているだけであるという議論もある。江口(2000, 182-183 頁)が指摘するように、Spafford(1992, pp. 44-45)は、これに対して次のような帰結主義的な議論をしている。使用されていないシステムは、システム外部の人間のためのものではなく、そのシステムを使う権限が与えられている人たちが、突然大量のデータを処理する必要が生じたりした場合のためにある。コンピュータを持っていない人が、使用されていないシステムを利用したとしたら、もともとのシステムに多大な負荷がかかり、必要なときに利用できなくなってしまうかもしれない。つまり、ハッカーが使用されていないシステムを利用することによって得られることより、そうすることによって失われることのほうが大きいのだ。

2.4 学生ハッキングの議論

ハッカーは何も害を与えていないし、何も変えておらず、システムがどのように動いているかを学んでいるだけであるという議論もある。しかし、コンピュータに関して学ぶということは、その原理的な側面を深く学ぶということであり、システムに侵入することとは無関係である。また、システムを「学んでいる」学生は、システムに侵入することによってどのような帰結をもたらすかを分かっていない。つまり、意図していないような大きな害を与える可能性がある。例えば、ハッカーが医療システムに侵入したとき、そのシステムを停止させてしまうかもしれない。この場合、患者が生命の危機にさらされる可能性がある。さらに、システムの管理者は、システムへの侵入者が単なる好奇心で侵入しただけであって何の害を及ぼす意図はないと仮定することはできず、最悪の事態を想定する必要がある。この場合、システムの管理者に多大な負担を強いることになり、何も害を与えないことにはならない(Spafford, 1992, p. 45)。

この議論も、帰結主義的なものである(江口, 2000, 184 頁)。明示的に述べると、ハッキング行為によってコンピュータのシステムがどのようになっているかを学ぶことができるという良い帰結より、ハッキング行為によってウェブサイトの管理者に多大な労力をかけるという悪い帰結のほうが上回るということになる。

2.5 社会を守る守護者の議論

システムに侵入することは、個人のデータを密かに監視する「ビッグ・ブラザー」的な行為を阻止する役割を果たしているという議論もある。確かに会社や政府によって個人データが不当に利用されている場合はあるかもしれない。しかし、システムに侵入することによって、そのような不正を是正できるかどうかは明らかではない。むしろ、個人データを不正利用していた当事者は、そうした侵入をきっかけに、個人データをどのように利用しているかについて以前より秘密にするようになり、より巧妙な個人データの不正利用が進むかもしれない(Spafford, 1992, pp. 45-46)。

帰結主義の観点からこの議論を述べると、ハッキング行為によって個人のデータを密かに監視する「ビッグ・ブラザー」的な行為を阻止することによって、個人のプライバシーが守られるという良い帰結より、ハッキング行為によって個人データの不正利用がより進むという悪い帰結のほうが上回る可能性があるということになる。

3. Manion & Goodrum(2000)の議論

3.1 市民的不服従とは

Manion & Goodrum(2000)は、市民的不服従の観点から、ハッキング行為を正当化する議論を行った。彼らの議論は、Spafford(1992)が取り上げた議論とは異なり、ハッキング行為全般を擁護しようとするものではなく、ハッキング行為は市民的不服従とみなされるときのみ正当化されるというものである。つまり、ハッキング行為全般ではなく、ある特定のハッキング行為を擁護しようとするものであった。

市民的不服従とは、不正な法律に非暴力的に抵抗するような行為である。これは、特定の不正な法律を破るという直接的な市民的不服従と、その法律の問題点に間接的に注意を向けさせる象徴的な市民的不服従に分けられる(Manion & Goodrum, 2000, p. 15)。例えば、レストランの座る場所を人種によって隔離する法律があったとしよう。そして、そのような法律は不正であるという動機のもと、この法律で禁じられている場所に、警官に連行されるまで座り続けたとする。これは直接的な市民的不服従である。また、この法律に抗議

するために政府の建物の前で座り込みを行ったとする。これは、象徴的な市民的不服従である。

また、市民的不服従の道具としてコンピュータを使った場合、電子的な市民的不服従とよばれる。これは、さらに二つに分けられる(Manion & Goodrum, 2000, p. 15)。一つは、市民的不服従を支援するためにコンピュータを使う場合で、例えば電子メールやウェブサイトを使って自分の意見を公表したりすることである。もう一つは、コンピュータを使うことが市民的不服従の行為そのものである場合で、例えば道徳的に不正な行為に関わっている機関のコンピュータシステムに不正侵入したりすることである。

さらに Manion & Goodrum(2000)は、Denning(2001, p. 241)による実行主義、ハッキング的実行主義、サイバーテロリズムという区別を採用している。実行主義とは、自分の政治的な主張を訴えるために、インターネットを通常のやり方で使用し、混乱を引き起こしたりしない立場のことである。ハッキング的実行主義は、実行主義とハッキング行為を結びつけたもので、自分の政治的な主張を訴えるという目的のもと、システムに侵入し通常の操作を妨害しようとするが､深刻なダメージを与えることが目的ではないような立場である。サイバーテロリズムは、人命を奪ったり、深刻な経済的損失といった大きな被害を意図した行動のことである。

こうした区別をもとに、Himma(2008)は、Manion & Goodrum(2000)による議論を次のようにまとめている。

> 市民的不服従は不正への抗議として正当化されるのだから、不正への抗議の方法として、ハッキング行為にコミットすることは許される。例えば、人権を侵害している法律に抗議するために、商業的な、もしくは政府の建物に座り込んだり、デモを計画することが許される場合に限り、そのような法律に抗議するために商業的もしくは政府のネットワークに侵入することは許される。したがって、ハッキング行為は政治的な動機がなければ許されるものではないが、電子的な市民的不服従、つまりハッキング的実行主義という政治的に動機づけられている行為であれば、道徳的に正当化される。(Himma, 2008, p. 196)

このように Manion & Goodrum(2000)による議論は、ある特殊な状況、つまり市民的不服従とみなすことができるような状況であれば、ハッキング行為は不正ではないという議論である。したがって、この議論で重要なのは、どのような条件においてハッキング行為を市民的不服従とみなせるのかということである。

市民的不服従を政治的な表現とみなすと、この行為を表現の自由という道徳的権利の行使として考えることによって、市民的不服従は直ちに道徳的に正当化されるようにみえるかもしれない。しかし、このような推論には次のような二つの問題点がある(Himma, 2008, pp. 196-197)。一つめの問題点は、X が p ということを表現する権利をもつということは、p を表現することが道徳的に許されるということを含意しないということである。例えば、人種差別的な考えを表現することは道徳的に許されないが、そのような考えを表現する権利はあるかもしれない。そもそも表現の自由というものは他人が自由に表現することを認めなければならないということを意味しているのであって、自分自身が何でも自由に表現するということが道徳的に許されるということは意味していないのだ。二つめの問題点は、そもそも市民的不服従は単なる表現ではなく、行為であるということである。何らかの行為を通して、自分の主張を表現しているのだ。したがって、市民的不服従は単なる表現の自由という道徳的権利の行使ではないのである。

一方、上の議論に基づき、市民的不服従を正当化することができないと結論することも妥当ではない。この議論は、表現の自由という道徳的権利の行使として、市民的不服従を正当化することが妥当でないということを示しているだけだからだ。しかし、以下の三つの理由より、不正な法律に従わないということが道徳的に許されることはめったにあることではない(Himma, 2008, p. 197)。一つめの理由は、民主主義の国家の市民は、市民的不服従という手段以外に、自分の意見を表明する様々な手段を持っているということである。二つめの理由は、民主主義は、どのような法律を法制化するかということに、全ての人が平等に関わるようになっているということである。自らが制定に関わっている法律に背くということは、民主主義という制度において与えられた権利を正当に行使しているとはいえない。三つめの理由は、法律は不正か不正でないかという単純な二項対立では捉え切れず、許容できる範囲で不正な法律もあるということである。例えば、税に関する法律は国民全員に対して完全に公平に課税しているとはいえないので、平等であるかどうかという観点からみると、完全に正しいとはいえない。しかし、そのことを理由に脱税をすることは道徳的に許されるわけではないだろう。以上の理由より、市民的不服従という行為が道徳的に正当化されることは、めったにあることではない。それにもかかわらず、Manion & Goodrum(2000)は、市民的不服従が道徳的に正当化されることがあると考えている。3.2 節で、彼らの議論を検討しよう。

3.2 市民的不服従が正当化される条件

Manion & Goodrum(2000)は、市民的不服従はどのような条件のもとで道徳的に正当化されると考えているのだろうか。帰結主義の観点から考えるならば、市民的不服従によって、もたらされるであろう帰結を検討しなければならない。市民的不服従という行為によってもたらされる良い帰結は、不正に注意を向けさせること、そしてそれに関する議論を喚起させるということであろう。これが、市民的不服従によってもたらされる悪い帰結を上回るとき、市民的不服従は正当化される。

Manion & Goodrum(2000, p. 15)は、ある行動が市民的不服従であるとみなされるために必要な条件を挙げている。

1. 人や物に危害を加えないこと。
2. 暴力的でないこと。
3. 個人的な利益のために行うのではないこと。
4. 倫理的な動機づけをもっていること。つまり、法律が不正であり、共通善を極端に損なうと強く確信していること。
5. 行動した結果に対する個人的な責任を受け入れること。

これらの条件は、市民的不服従によってもたらされる悪い帰結をできるだけ最小限にするための条件と考えられる。暴力的であれば、人や物に危害を加えることになるので、1番目の条件は2番目の条件を含意している。また、倫理的な動機づけをもって行う行為は、個人的な利益のために行う行為ではないだろう。つまり、4番目の条件は3番目の条件を含意している。そこで、本稿では、1番目、4番目、5番目の条件を検討する。

まず、無関係な人にどれくらい害を与えるかという1番目の条件から考えよう。これは、標的が公的であるか、私的であるか、商業的であるかに依存する(Himma, 2008, pp. 201-202)。例えば、大量のデータを送りつけシステム障害を起こさせるサービス妨害攻撃（DoS）を商業的なウェブサイトに仕掛けた場合、ビジネス上の損失を与えることになり、場合によっては従業員の解雇につながるかもしれない。また、個人のウェブサイトにサービス妨害攻撃を仕掛けたら、表現の自由を侵害することになるし、個人のコンピュータのファイルにアクセスしたら、プライバシーを侵害することになる。公的なウェブサイトへの攻撃では、こうした損失は生じない。しかし、損失を全く与えないということはない。例えば、2011年11月9日、自治体向けに提供している電子申請システムにサービス妨害攻撃が仕掛けられ、いくつかの自治体の電子申請システムが利用できなくなった(2)。商業的なウェブサイトに比べて害は少ないかもしれないが、この攻撃によっても、このシステムの利用

者に不便をかけるという害を与えている。このように、害を与える程度は、標的が公的であるか、私的であるか商業的であるかに依存するものの、いずれの場合も害を与えている。

また、どれくらい害を与えるかということは攻撃の種類にも依存する。そのサイトにアクセスできなくするサービス妨害攻撃（DoS）に比べて、不正侵入を行いウェブ上にメッセージを書きこむといった電子的落書き（E-graffiti）は害が少ないようにみえる。特に、重要なサービスや情報を提供していないウェブサイトの文字を少し変えたとしても、害はないようにみえる。実際、Manion & Goodrum(2000)は、このような行為は害を与えていないと考えている。しかし、Denning(2008, p. 421)が指摘しているように、これは間違いである。サービス妨害攻撃に比べると、害は少ないかもしれないが、落書きを修復するためにシステムの管理者は手間を取ることになり、間接的に危害を加えている。また、2.4 節で述べた「学生ハッカーの議論」に対する Spafford(1992)による反論のように、システムに侵入し落書きをしただけのつもりであっても、思いもよらない危害を与える可能性もある。ハッキング的実行主義に関わる人は、ハッキング行為によって自らの主張を表明することによって得られる良い帰結が、こうした悪い帰結を上回ることを示す必要がある。しかし、このことを示したとしても、それだけでは不十分である。行動した結果に対する個人的な責任を受け入れるという 5 番目の条件もみたす必要があるからだ。

そこで、5 番目の条件を考えよう。まず、自分の行動に対する責任を主張することと、自分の行動が引き起こす法的な帰結を受け入れることは違うということに注意すべきである(Himma, 2008, p. 203)。例えば、偽名をもちいて行動したり、ある集団の一員として行動することにより、自分の行動による法的な帰結を受け入れることなく、自分の行動に対して責任をもっていると主張することは可能である。Manion & Goodrum(2000, p. 15)は、自分の行動の法的な帰結を受け入れ牢屋に入った人物の例を挙げているので、彼らが念頭においているのは後者の方である。つまり、ハッキング的実行主義に携わるならば、匿名であってはならない。

匿名の相手に攻撃されると、システムの管理者はどのような相手に攻撃されているかわからないので、インターネットのセキュリティをより心配するようになる。そのため、そのコストが増大する。また、より創造的な目的のために使うことができた資源が、コンピュータのセキュリティのために使われることになり、創造的な活動が制限される。このような意味において、匿名による攻撃は、社会に損失をもたらす。したがって、帰結主義の観点から考えても、自分の名前を明らかにした上で、自分の行動が引き起こす法的な帰結を受け入れるということは必要である。しかし、このように行動したとしても、これでもまだ不十分である。電子的市民的服従に携わる人は倫理的な動機をもつ必要があるからだ。

そこで、電子的市民的服従に携わる人に倫理的に動機があるかどうかという 4 番目の条件を最後に考えよう。倫理的な動機があるかどうかという区別は、ハッキング的実行主義とサイバーテロリズムを区別する上で重要である。また、帰結主義の観点からみると、この条件は以下の意味において重要である。システムの管理者は、システムへの侵入があった場合、侵入者の動機を知らなければ、2.4 節でも論じたように、最悪の事態を想定する必要がある。例えば、上で述べたように、2011 年 11 月 9 日自治体向けに提供されている電子申請システムにサービス妨害攻撃が仕掛けられたが、攻撃が仕掛けられた時点で、誰がどのような動機で攻撃を仕掛けたのかは不明であった。この場合、システムの管理者はあらゆる可能性を考慮しなければならない。しかし、侵入者の動機が明確であれば、システムを破壊したり、機密情報が盗まれたりするといった最悪の事態を想定する必要はなくなる。つまり、システムの管理者に多大な負担をかけるという悪い帰結を避けることができる。この際、ハッカーは倫理的な動機をもつだけでなく、それを明確にする必要もある。

例えば、Manion & Goodrum(2000, p. 16)は、倫理的な動機をもとに行動したハッキング的実行主義の例として、「民衆の手に再び力を」というスローガンを掲げたハッカーを挙げている。しかし、Himma(2008, p. 206)が指摘しているように、このスローガンは非常に曖昧であり、これだけから正確に意図することを汲み取ることは難しい。そのため、結局管理者は最悪の場合を想定しなければならないだろう。

また、2.1 節で扱った「情報はフリーである」というスローガンも考えてみよう。これもハッカーによってしばしば主張される見解である。ハッカーは、この主張によって「有用なプログラムは自由に使え、無料で配布できるようになるべきである」ということを述べているだけであり、「クレジット会社や、国防上重要な機密やわたしの個人的な情報が皆によってアクセス可能になるべきである」と主張しているわけではないかもしれない(江口, 2000, 179 頁)。しかし、「情報はフリーである」というスローガンのみから、このハッカーの意図を汲み取ることは難しい。つまり、2.1 節で述べたように、プライバシーや情報の正確さに対する懸念を払拭することは難しく、管理者は最悪の場合を想定しなければならないだろう。

したがって、ハッキング実行主義者は、自分の行為の動機を曖昧ではなく明確にしなければならない。この条件をみたすためにハッキング的実行主義者が行うべきことは、自らの倫理的動機に関して極力多くの人と議論することである。もちろん、他人と議論することなしに、自分の倫理的動機を明確にすることができる人もいるだろうが、そうした人は稀であろう。多くの人は他人と議論することによって、自分の動機を明確にすることができる。しかし、こうしたことを行った後、ハッキング行為を行う意味はあるのだろうか。

そもそも市民的不服従としてのハッキング行為の目的は、不正に注意を向けさせ議論を喚起することであった。ハッキング行為を正当化するために、多くの人と議論し自らの動機を明確にすることによって、多くの場合すでにその目的を達しているといえる。この目的を達しているにもかかわらずハッキング行為を行うということは、不正に注意を向けさせ議論を喚起するという倫理的な動機をもたないでハッキング行為を行うことである。これは、倫理的な動機を持たなければならないという 4 番目の条件に反する。そうした意味で、ハッキング行為が正当化されることは、ほとんどない。

4. おわりに

本稿では帰結主義の立場に立った上で、ハッキング行為の帰結に注目し、どのような条件のもとでハッキング行為が正当化されるのかという問題を考えてきた。2 節でみたように、Spafford(1992)が取り上げた議論はハッキング行為全般を正当化しようとする議論であり、Spafford(1992)はそれらの議論を批判した。一方、3 節でみたように、Manion & Goodrum(2000)は、ハッキング行為全般ではなく、市民的不服従として考えられるハッキング行為を正当化しようとし、そのための条件を考察していた。この意味で、Manion & Goodrum(2000)は、Spafford(1992)が取り上げた議論より弱い主張をしている。

本稿では、Manion & Goodrum(2000)がハッキング行為を市民的不服従とみなすために必要であると考えた条件を検討した。市民的不服従としてのハッキング行為の目的は、不正に注意を向けさせ議論を喚起することであった。しかし、3.2 節の最後で論じたように、このようなハッキング行為が正当化されるためには、まずその動機について議論しなければならない。つまり、市民的不服従としてのハッキング行為が正当化されるために必要な準備の段階で、その行為の目的にあたることを行う必要がある。したがって、その準備が終わった段階で、多くの場合すでにハッキング行為を行う目的は達している。この目的を達しているにもかかわらずハッキング行為を行うということは、不正に注意を向けさせ議論を喚起するという倫理的な動機をもたずにハッキング行為を行うことになる。この場合、Manion & Goodrum(2000)がハッキング行為を市民的不服従とみなすために必要であると考えた条件をみたさない。このような意味で、ハッキング行為が正当化されることは皆無に近い。

註

(1) 2011 年 8 月 16 日毎日新聞東京夕刊「シリコンバレー精神：IT 先駆者の文化革命」による。
(2) 2011 年 11 月 10 日毎日新聞東京夕刊による。

文献

Denning, D. E. (2001). 'Activism, hacktivism, and counterterrorism', in J. Arquilla and D. Ronfeldt (eds.), *Networks and Netwars* (pp. 229-288), Santa Monica: RAND .

——— (2008). 'The ethics of cyber conflict', in K. E. Himma (ed.), *The Handbook of Information and Computer Ethics* (pp. 407-428), New Jersey: John Wiley and Sons, Inc.

江口聡 (2000). 「システム侵入の倫理的問題」, 越智貢・土屋俊・水谷雅彦編, 『情報倫理学　電子ネットワーク社会のエチカ』(171-187 頁), ナカニシヤ出版.

Himma, K. E. (2008). 'Ethical issues involving computer security: hacking, hacktivism, and counterhacking', in K. E. Himma (ed.), *The Handbook of Information and Computer Ethics* (pp. 191-217), New Jersey: John Wiley and Sons, Inc.

Manion, M. and Goodrum, A. (2000). 'Terrorism or civil disobedience: toward a hacktivist ethics', *Computer and Society, June*, 14-19.

Moor, J. H. (2001). 'The future of computer ethics: you ain't seen nothin' yet!'. *Ethics and Information Technology, 3*, 89-91.

Spafford, E. (1992). 'Are computer hacker break-ins ethical?', *Journal of Systems Software, 17(1)*, 41-48.

〔日本大学生産工学部・科学哲学〕